Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.-6. (canceled)

7. (currently amended) A restricted data format method for a network infrastructure copy protection system, comprising:

receiving a digital content file for transmission across a distributed computer network;

examining data comprising the content file to determine whether the content file includes a restricted data format, the examining performed within the distributed computer network, and wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format;

transmitting the content file when data comprising the content file does not include the restricted data format; and

blocking transmission of the content file when data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver.

8.-10. (canceled)

11. (original) The method of Claim 7 wherein the distributed computer network is the Internet.

12. (original) The method of Claim 7 wherein the examining is performed by a plurality of routers within the distributed computer network.

13. (original) The method of Claim 7 wherein the examining is performed by a plurality of cache engines within the distributed computer network.

14.-16. (canceled)

17. (currently amended) A network infrastructure protection method for detecting and denying transmission of restricted data formats, comprising:

receiving a digital content file for transmission across a distributed computer network;

using at least one router configured to log digital signatures related to the digital content file to maintain a record for the digital content file and the related digital signatures, the record including the related digital signatures, examining data comprising the digital

content file to determine whether the digital content file comprises a restricted data format, wherein the digital content file is free of a digital signature, the examining performed within the distributed computer network, and wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format;

transmitting the digital content file when the data comprising the digital content file does not include the restricted data format; and

blocking the transmission of the digital content file when the data comprising the digital content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the digital content file to a receiver.

18.-20. (canceled)

21. (currently amended) A network device comprising:

a bus;

computer readable memory units connected to said bus;

one or more processors coupled to said bus said computer readable memory units for executing a digital signature method for a network infrastructure copy protection system, comprising:

applying a digital signature to a digital content file;

examining the digital content file to determine whether the digital content file includes the digital signature, wherein the examining is performed within the distributed computer network;

transmitting the digital content file when the digital content file includes the digital signature; and

blocking transmission of the digital content file when the digital content file does not include the digital signature to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the digital content file to a receiver; and

blocking transmission of the digital content file when the data comprising the content files is a restricted data format to prevent unauthorized downloading of copyrighted material ,wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format.

22. (previously presented) The device of Claim 21 wherein the digital signature is configured to identify the sender of the digital content file.

23. (previously presented) The device of Claim 21 wherein the digital signature applied to the content file within the distributed computer network is logged to maintain a record for the content file and the digital signature when the content file is transmitted across the distributed computer network.

24. (previously presented) The device of Claim 21 wherein the distributed computer network is the Internet.

25. (previously presented) The device of Claim 21 wherein the examining is performed by a plurality of routers within the distributed computer network.

26. (previously presented) The device of Claim 21 wherein the examining is performed by a plurality of cache engines within the distributed computer network.

27. (currently amended) A network device comprising:

one or more network interfaces;

computer readable memory units connected to said one or more network interfaces;

one or more processors coupled to said bus said computer readable memory units for executing a method for detecting and denying transmission of restricted data formats, comprising:

receiving a digital content file for transmission across a distributed computer network;

using at least one router configured to log digital signatures related to the digital content file to maintain a record for the digital content file and the related digital signatures, the record including the related digital signatures, examining data comprising the digital content file to determine whether the digital content file comprises a restricted data format, wherein the digital content file is free of a digital signature, the examining performed within the distributed computer network, and wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format;

transmitting the digital content file when the data comprising the digital content file does not include the restricted data format; and

blocking the transmission of the digital content file when the data comprising the digital content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the digital content file to a receiver.

28.-29. (canceled)

30. (currently amended) A restricted data format system for a network infrastructure copy protection system, comprising:

means for receiving a digital content file for transmission across a distributed computer network;

means for examining data comprising the content file to determine whether the content file includes a restricted data format, the examining performed within the distributed computer network, and wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format;

means for transmitting the content file when data comprising the content file does not include the restricted data format; and

means for blocking transmission of the content file when data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to a receiver.

31. (currently amended) A network infrastructure protection system for detecting and denying transmission of restricted data formats, comprising:

means for receiving a digital content file for transmission across a distributed computer network;

means for using at least one router configured to log digital signatures related to the digital content file to maintain a record for the digital content file and the related digital signatures, the record including the related digital signatures, examining data comprising the digital content file to determine whether the digital content file comprises a restricted data format, wherein the digital content file is free of a digital signature, the examining performed within the distributed computer network, and wherein the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format;

means for transmitting the digital content file when the data comprising the digital content file does not include the restricted data format; and

means for blocking the transmission of the digital content file when the data comprising the digital content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to the transmission of the digital content file to a receiver.